F–16s patrolling skies over Washington.

148th Fighter Wing (Dean Kuhlman)

# Strengthening Security at Home

*By* MICHÈLE A. FLOURNOY

The events of September 11, 2001, pierced the sense of invulnerability that most Americans had come to expect. Although the feeling of security at home waxed and waned with the perils of the Cold War—from duck-and-cover drills in the 1950s to détente in the 1970s—an expectation of being removed from any direct threat of war became common after the fall of the Soviet Union. As the sole superpower, the United States pursued its interests as a nation at peace. If the Persian Gulf War warned that were still threats around the world, it also reinforced the idea that America would fight its wars far from home. As one Pentagon wag quipped in the 1990s, the Armed Forces only played away games.

In the decade following Desert Storm, some defense analysts began to focus on asymmetric threats that could be directed at the homeland. At the

**Michèle A. Flournoy is currently a senior advisor at the Center for Strategic and International Studies and has served as Principal Deputy Assistant Secretary of Defense for Strategy and Threat Reduction.**

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2002** | | **00-00-2002 to 00-00-2002** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Strengthening Security at Home** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**National Defense University,Institute for National Strategic Studies,Fort Lesley J. McNair,Washington,DC,20319** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **8** | |

same time the Clinton administration initiated various actions to help Federal, state, and local governments enhance their ability to defend against and coordinate responses to attacks on the United States. But Americans remained either unaware or unconvinced of any threat even after the attack on the World Trade Center in 1993.

In the wake of the worst terrorist attack in the history of the Nation, homeland security has become the top priority. Before September 2001 there was a growing commitment among many government officials to guard against such threats to the United States. Since then there has been an urgent public demand and an unprecedented political will to do whatever is necessary to enhance homeland security as quickly as possible. Congressional approval to give the President $40 billion in an emergency supplement—twice the sum requested—was indicative of the new mood.

But a year after this wake up call, the United States still lacks a homeland security strategy to manage risk and guide resource allocation. Although Congress is debating how to organize for homeland security, no decisions have been made on which threats require attention, what programs should receive a priority, and how resources must be allocated. Given this policy vacuum, there is an urgent need for an integrated, strategy-driven homeland security program.

## Prevention, Protection, Response

Homeland security means preventing, deterring, preempting, and defending against attacks against the United States, and managing the consequences of any attack. Inherent in this definition are three broad-based and enduring objectives that must underpin a new national strategy. The first is preventing attacks. This is central to the open, democratic, market-based American way of life. Prevention involves countering threats before they become manifest as far from the Nation's borders as possible. This can range from efforts mounted with allies to roll up terrorist networks or denying access to weapons of mass destruction to immediate actions inside the United States to prevent terrorists from renting crop-dusters. Prevention is proactive, requiring offensive action to destroy or neutralize threats before an attack occurs. It involves "shaping the security environment to avoid or retard the emergence of threats to the United States," which can only be achieved by action abroad.[1] In this regard, the Departments of State and Defense, allies, and law enforcement agencies overseas play a significant role. In the final analysis, the major element of prevention is detecting threats in advance, with enough specificity and warning to take preventive action.

**decisionmakers must anticipate the kinds of attacks that might occur and details on their nature, location, and timing**

To deflect attacks, decisionmakers must anticipate the kinds of attacks that might occur and details on their nature, location, and timing. This requires good intelligence collection and analysis and, in most cases, substantial sharing of information across national and agency lines.

Because not every threat can be prevented, the goal must be to minimize the likelihood that the most serious types of attack could be mounted successfully. As the Secretary of Defense said, "Our victory will come with Americans living their lives day by day, going to work, raising their children, and building their dreams as they always have—a free and great people."[2] The fact that Federal law enforcement and intelligence agencies have averted such attacks in the past by acting rapidly on specific indications is proof that a degree of prevention is possible.

The second objective of homeland security is enhancing the capability of the United States to protect itself against attack. This includes strengthening defenses against a range of threats that might come from a variety of directions against any number of targets.

Essential to the protection of American citizens is a capability to defeat or neutralize enemy action once an attack is launched. A range of capabilities that includes domestic law enforcement, intelligence, military, and public health organizations will be needed to mount effective barriers to such attacks whether they involve immediate responsive defense against either aircraft or missiles, a rapidly instigated search to find and foil a terrorist cell, or day-to-day security measures to patrol borders and protect critical infrastructure. This aspect of homeland security is particularly complex because of the variety of acknowledged threats, the increasing sophistication of known terrorists, and the ability of subversive elements to adapt their mode of operations to new countermeasures and exploit weaknesses in existing protective systems.

Efforts must focus not only on ensuring that terrorists can never again hijack airliners and fly them into skyscrapers. The United States must guard against planes, missiles, vehicles, ships, chemical or biological agents, nuclear materials in urban areas, and cyber and physical attacks on critical infrastructure. Both lethal and non-lethal disruptive threats demonstrate the complexity of the problem and range of participants in the public and private sectors who should be involved in protecting the homeland. This diversity highlights the need to prioritize. The United States cannot afford to give equal weight to defending against every conceivable threat scenario.

The third objective is improving the ability to manage the consequences of an attack. First, there must be a forceful capability to guarantee public safety; continuity of government; command, control, and communications; and essential services. Effective consequence management is central to maintaining public confidence and reducing the impacts of terrorism. As seen on September 11, first responders such as firefighters, police, and emergency rescue teams are often the most critical elements of consequence management. They should

Ground zero.

Fleet Combat Camera, Atlantic (Aaron Peterson)

The Pentagon, September 11.

U.S. Marine Corps Photolab (Jason Ingersoll)

have the assets and training to coordinate their activities under extraordinary conditions, such as the use of weapons of mass destruction.

Second, the United States must be able to minimize disruption and restore the infrastructure rapidly in the immediate aftermath of any attack. This might involve restoring telecommunications service, repairing energy production and distribution systems, or providing alternative means and routes of communication and transportation. Hardening potential targets, developing contingency plans, and building a degree of redundancy into key systems will be critical to rapid restoration.

Third, the Federal Government must be prepared to quickly stabilize financial markets and manage economic consequences of an attack. This should involve agencies such as the Treasury Department and Federal Reserve System working in partnership with the private sector.

Fourth, Federal, state, and local agencies as well as nongovernmental organizations must provide immediate assistance to attack victims and affected communities. Central to protection and response are advanced planning, exercises, and simulations that identify problems and coordinate efforts among government and private sector representatives.

## The Long Pole in the Tent

Intelligence is indispensable in the global war on terrorism. However, given the nature of the enemy, there is no assurance that the quality of intelligence on organizations like al Qaeda will notably improve without institutional changes and a sustained effort by the intelligence community. As a flat organization composed of small cells of individuals in more than sixty countries, al Qaeda has demonstrated its ability to employ a range of communications, from low-tech means such as face-to-face meetings to high-tech devices such as encryption. When communications have been intercepted, it has been agile in changing its modus operandi.

Terrorist organizations do not rely on the kind of assets that make other intelligence targets such as governments easier to penetrate. Thus national technical means of collection—satellites, electronic eavesdropping, and surveillance aircraft—are less effective. Moreover, extremism not only motivates recruits and cements otherwise loose networks, but makes them almost impossible for Western agents to infiltrate. Because of their strong ideological convictions, members of these groups are unlikely to defect even if offered incentives. Given these factors, the campaign against terrorism may pose the biggest intelligence challenge since the Cold War.

Homeland security presents a set of requirements that call for an understanding of the types of attack that various terrorist organizations are able to launch. If indicators suggest that an attack is imminent, authorities need specific warning on its location and type to enhance law enforcement, security, and consequence management. Such insight is unlikely to emerge without a synthesis of relevant information across bureaucratic lines into a coherent, timely picture.

One of the greatest challenges to homeland security is enhancing situational awareness—the ability to know what terrorists are doing inside national borders—without becoming a police state. Consider the fact that perpetrators of the September 11 attacks

lived, prepared, and hid in America for several years but went undetected. This lapse occurred because the intelligence community did not collect and evaluate the right information. There is a need to redesign collection and analysis strategies within the intelligence and law enforcement communities.

In addition, relevant bits of information were available in various agency files but remained needles in a proverbial haystack of intelligence data. This points to the need for new technologies to organize, store, and retrieve data already collected. Another concern is that agencies may have identified key elements of information yet failed to correlate them to present the larger picture. This argues for better data sharing across agency lines. But such efforts raise the specter of intelligence activities within U.S. borders, which has long been seen as a threat to civil liberties.

**intelligence sharing must be overhauled to enable rapid, effective fusion and ensure situational awareness**

The campaign against terrorists requires coming to terms with the question of basic rights. Creating situational awareness will call for new methods of lawful surveillance of both citizens and foreigners living in America, while establishing adequate oversight mechanisms to ensure that they are not misused. In short, a better job should be done to track and find terrorists on American soil while protecting our fundamental liberties.

Since better intelligence is indispensable, it is imperative that the United States act quickly and prudently to address the most serious problems in the counterterrorism campaign. For a start, the President should require an interagency assessment to identify shortfalls in intelligence policy, capabilities, practices, and resources that could hamper effectiveness. Based on a comprehensive assessment, the administration must develop a multi-year action plan.

Second, the President should assign a high priority to strengthening bilateral intelligence-sharing and cooperation with countries that have the most to offer on the terrorist organizations of greatest concern. After September 11, such arrangements are defining political issues in relations with many nations. A central diplomatic goal must be to broaden and deepen these arrangements as a cornerstone of bilateral relations with key countries. This should include continuing to seek greater cooperation in surveillance of the financial transactions of terrorist organizations.

Third, Congress should increase resources devoted to the intelligence community in general and the global war on terrorism in particular. This will be essential in addressing critical shortfalls in areas such as human intelligence, covert operations, analysts, linguists, area specialization, and the integration of new technologies, especially with regard to information management.

Fourth, the guidelines and processes for intelligence sharing must be overhauled to enable rapid, effective fusion and ensure situational awareness. This must occur not only on the national level but also among Federal, state, and local agencies. American lives are on the line, and there is no excuse for bureaucratic infighting that compromises the ability to exploit available intelligence.

Such initiatives will require a shift from a case file approach of domestic law enforcement to more fundamental and proactive data analysis. It will also demand substantial investment in data correlation and analysis capabilities, as well as sharing data across bureaucratic lines. Improving the ability to correlate data will mean reevaluating rules that govern collecting intelligence on private citizens and others living in this country. Specifically, the United States must organize combined-agency investigation centers supervised by officials who are named by the court authorized under the Federal Intelligence Surveillance Act. These officials would be real-time privacy ombudsmen to guard against the inappropriate use of new investigative techniques.

Fifth, intelligence and law enforcement agencies must conduct more red team assessments to better anticipate what types of attack terrorists might contemplate and how to respond. Though imperfect, such efforts can expose gaps in thinking and shortcomings in preparation.

Finally, the intelligence community cannot be expected to solve every problem on its own. It must pursue public-private partnerships to engage the best expertise to surmount technological hurdles. Particular investment must be made in new technologies to store and retrieve information. In the wake of September 11, it should not be hard to find private sector partners. More broadly stated, the intelligence community should seek to leverage the diversity and openness of America, engaging experts and linguists outside the Government through outreach and outsourcing.

The intelligence and law enforcement communities are recognized as crucial and in need of resources and reform. Nothing will be more important to fighting terrorism and homeland security than meaningfully improving the capabilities and performance of these two communities.

## Preparing for the Worst

As the United States develops a strategy for homeland security, it should pay attention to the greatest threats to its way of life: bioterrorism and attacks on critical infrastructure.

While chemical agents could produce hundreds of thousands of casualties, an attack using biological pathogens could cause millions. It is well established that al Qaeda has sought biological means of attack and has contacts with states that have biological weapons programs. The anthrax attacks after September 11 ended the debate about whether or not an individual or small group can obtain and use biological agents.

The good news is that biological pathogens are generally difficult to weaponize; it is hard to produce them in large quantities and format their dispersal to cause mass casualties. The bad news is that dedicated terrorists would need only a small quantity of a highly contagious pathogen such as

smallpox to create a mass-casualty event. Every infected person would be a walking biological weapon. This danger is magnified in a mobile society. Local bio-attacks could turn into a national crisis that could be crippling. The Nation must therefore give highest priority to keeping pathogens out of the hands of terrorists and enhancing its ability to deal with such attacks.

Security measures at U.S. and foreign facilities have not been adequate to prohibit theft of dangerous pathogens. Samples of some pathogens such as smallpox are kept under tight control in America, whereas others like anthrax are stored in labs under minimal security. Across the former Soviet Union, literally tons of biological weapons agents are housed in nonsecure facilities.

**an active, sustained partnership between the public and private sectors will be essential in the case of bio-defense**

In addition, we are ill-prepared to manage the aftermath of a large-scale bioterrorism attack. The United States has neither sufficient stockpiles of vaccines and antibiotics nor means to rapidly distribute them. It also lacks adequate cadres of first responders trained and equipped to deal with such a crisis. The Government also needs management strategies, plans, and information systems. Senior leaders simply would not get the intelligence and expert advice required to make informed decisions. Federal and state officials could find themselves in the untenable position of using force to constrain the movement of citizens absent a viable means to contain a crisis. This may endanger civil liberties and also test decisionmakers. Indeed, the less adequate the response to bioterrorism, the greater both the likely panic and the threat to basic freedom.

Working with members of Congress and state and local government officials, the President should undertake a public-private initiative to enhance national capabilities. This effort must focus on the public health system to limit the catastrophic potential of bioterrorism.

Substantial investments are needed to strengthen public health expertise, infrastructure, and early warning systems. New approaches must be developed to deal with the diseases that might be used as weapons of terror, especially stockpiling vaccines and antibiotics, strengthening national and regional distribution, and researching and developing other means of facilitating rapid disease control such as easily deployable diagnostic tools using new biotechnologies. Administration and congressional action to create a stockpile of hundreds of millions of doses of smallpox vaccines is a step in the right direction, but much more needs to be done to safeguard against other pathogens. Particularly important will be developing an appropriate regulatory process to ensure the safety of vaccines and antibiotics as well as providing medical and pharmaceutical industries with incentives such as liability protection to rise to this national challenge.

This initiative must also include the development and implementation of a robust security protocol to protect laboratories that store pathogens which could be used in terrorist attacks; an extensive program of analysis, simulations, and exercises to improve knowledge of such threats and identify and prioritize shortfalls; development of detailed plans and decisionmaking protocols, including clarification of jurisdictional issues between Federal and state entities; and development of information systems on all levels to better manage such events.

In addition, the United States must deal with the legacy of biological weapons in the former Soviet Union through cooperative threat reduction programs. This effort should reinvigorate and reorient the Biological Weapons Convention to take into account new bioterrorism threats. Only in preparing for the worst case can the potential consequences be limited.

The security of critical infrastructure—physical assets and cyber-based systems essential to the minimal operations of the economy and bureaucracy—is another urgent challenge in addressing the risks and consequences of terrorism. Widespread disruption and panic would quickly ensue if an aircraft breached the containment structure of a nuclear power plant, a major urban power plant was shut down, or the computer system of the New York Stock Exchange was sabotaged.

Between 80 and 90 percent of critical infrastructure is either owned or operated by private firms. It includes telecommunications, electrical power systems, gas and oil distribution, banking and financial institutions, transportation, water resources, and emergency services. In the new age of information technology much critical infrastructure has become automated, bringing efficiencies but also vulnerabilities, including susceptibility to cyber attack. An active, sustained partnership between the public and private sectors will be essential in the case of bio-defense.

Significant progress has been made, including the organization of Information Sharing and Analysis Centers by the Government in partnership with the private sector for addressing electronic threats, vulnerabilities, incidents, and solutions. But to date such efforts have largely focused on cyber-based rather than physical threats. Given that terrorist groups like al Qaeda have displayed interest in inflicting highly visible mass-casualty events, cyber strikes may not be a preferred mode of attack. The Bush administration should focus on physical vulnerabilities and threats in various sectors in its efforts to improve critical infrastructure protection.

The United States needs not only new threat and vulnerability assessments, but also a clear delineation of various responsibilities and authorities for the security of critical infrastructure. For example, who is responsible for security at over 100 nuclear power plants? The utility companies who operate the plants, local law enforcement agencies, or the National Guard under state control? These issues must be clarified through consultations between Federal, state, and local governments and industry. Private firms will have a particularly important role,


Providing security in Salt Lake City.

151st Air Reserve Wing (Mark Savage)

ranging from designing new facilities to better withstand attack, to enhancing physical security systems at existing facilities, to bringing relevant technologies and products to market.

## Towards Homeland Security

Congress is scrutinizing the proposal for a department of homeland security, but regardless of the organizational structure that emerges, the challenges outlined above require that the Nation take five interrelated steps. First, it must conduct a thorough interagency assessment of possible dangers to the homeland, considering different kinds of threats and their consequences. Second, based on that assessment, it must develop a national strategy that articulates priorities for resource allocation—essentially where to place the emphasis and how to accept or manage a degree of risk. Third, it must create an interagency program review and budget process to integrate and prioritize homeland security efforts on the national level. Fourth, it must establish a program to simulate and train decisionmakers. Finally, it must develop operational concepts to enhance homeland security. Only these steps can enhance national security at an acceptable cost.

*Interagency threat assessment.* The first step is tasking the Homeland Security Advisor to lead a comprehensive interagency assessment of current and future threats. The objective would be to develop a framework for understanding potential threats and establishing short-, mid-, and longer-term goals. Participants should include the intelligence agencies; Federal Bureau of Investigation; Departments of Defense, Treasury, Transportation, Commerce, and Health and Human Services; and Centers for Disease Control and draw on open as well as internal information sources.

To make the appraisal a living process rather than a one-time exercise, the President should establish a new terrorism assessment unit in the Office of Homeland Security designed to think like terrorists and study ways security could be breached. This must not be an unbounded exercise of human imagination, but rather a disciplined review of terrorist doctrine and techniques, intelligence assessments, and goals and effects sought by terrorist groups. The unit should draw on research as well as unconventional sources. Its aim must be to shape the strategy and programs of departments and agencies that share the homeland security mission.

*National risk management strategy.* Next, the President should task the Homeland Security Advisor to conduct an interagency review to define and prioritize objectives, articulate a strategy to meet those objectives, and develop a concept of operations that assigns responsibilities to specific agencies and actors for executing the strategy. While this is the charter of the Homeland Security Advisor, and there has been much talk of developing a national strategy, no rigorous interagency process appears to be underway. This planning process must build on the threat assessment described above and include an assessment of capabilities to deal with priority threats. The objective should be to provide policy guidance and prioritize shortfalls in national capabilities.

Informed by a strategy review, the Homeland Security Advisor should develop a multi-year interagency action plan. The plan must specify short-term actions to be taken on a priority basis, long-term investments to enhance critical capabilities, and a clear division of labor, including lead agency responsibility for specific areas and actions. This plan should be issued by the President to guide resource allocation. It must be a living document that is annually revised. The development process must include input from all Federal agencies responsible for homeland security, as well as consultation with state and local agencies and actors. Such an integrated action plan will be critical to getting the highest returns on an investment totalling billions of dollars.

*Strategy-driven program and budget review process.* Once the plan is in place, the advisor should establish a rigorous program and budget review process which annually reviews activities and

Marines on Capitol Hill.

U.S. Marine Corps (Bryant V. Cox)

expenditures of relevant agencies in light of multi-year requirements. The review must provide a mechanism for enforcing Presidential priorities. White House backing will be essential.

The Homeland Security Advisor must also fully integrate Federal programs and plans with state and local governments and aid those authorities in enhancing homeland security capabilities. Because state and local governments are likely to be the first to respond, they will bear the lion's share of responsibility in implementing decisions made in Washington. They will feel the impact of any attack most acutely. These constituencies will have to be included in decisions to strengthen security at home. The same situation is true within the private sector, particularly firms involved in operating or securing critical infrastructure.

*Rigorous simulation and training.* The Office of Homeland Security must institute gaming or simulation of homeland security scenarios. Such simulations can reveal discontinuities in plans for future events, offer insights into complex problems that can't be learned from reports, establish operational working relationships among players in peacetime that are crucial for communication in crises, help organizations to surmount turf battles by recognizing what can be done as well as what various organizations bring to the table, and detect shortfalls in processes and capabilities that should be addressed. Comprehensive simulation and training must include periodic sessions for the President and cabinet as well as subcabinet and working-level officials in key positions.

*Develop new operational concepts.* Finally, the Office of Homeland Security should form an advanced concepts office that can develop approaches which bridge discontinuities and address shortfalls identified in simulations and training. It could use current research techniques to identify alternative operational concepts and provide guidance on capabilities to meet priority requirements.

Homeland security is front and center in America's consciousness, and it is likely to remain so, especially if further attacks occur. Unlike the Gulf War or even the decades of the Cold War, fighting terrorism will not have a clear endpoint. Rather, it will be similar to the wars on crime and drugs. Since intractable problems can't be eliminated, victory becomes a matter of reducing risks to an acceptable level. In sum, the realities of homeland security require the Nation to think about conflict in different ways and overcome its varied challenges.

The Federal Government in partnership with state and local agencies and the private sector must enhance homeland security to win the global war on terrorism. This effort must be started by conducting a comprehensive threat assessment and developing a national strategy and program that outlines clear priorities for investment. It must adopt ways of doing business to integrate policies, programs, and budgets across bureaucratic lines on the national, state, and local levels as well as the private sector. This will require both political will and leadership on the part of elected officials and historic levels of public support. But meeting this challenge is not an option; it is imperative for the Nation to prevail in this fight against terrorism. **JFQ**

NOTES

[1] Michael Dobbs, "Homeland Security: New Challenges for an Old Responsibility," *Journal for Homeland Security* (March 2001), http://www.homelandsecurity.org/journal/Articles/Dobbs.htm.

[2] Donald Rumsfeld, "A New Kind of War," *The New York Times*, September 27, 2001, p. A21.